(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
24. Juli 2003 (24.07.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/060721 A2

(51) Internationale Patentklassifikation[7]: G06F 12/00

(21) Internationales Aktenzeichen: PCT/IB02/05481

(22) Internationales Anmeldedatum:
12. Dezember 2002 (12.12.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 64 422.1 29. Dezember 2001 (29.12.2001) IB

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von DE, SI, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Anmelder *(nur für DE)*: **PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BUHR, Wolfgang** [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MUELLER, Detlef** [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Anwalt: **PETERS, Carl, H.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR WRITING NV MEMORIES IN A CONTROLLER ARCHITECTURE, CORRESPONDING COMPUTER PROGRAM PRODUCT AND COMPUTER-READABLE STORAGE MEDIUM

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUM BESCHREIBEN VON NV-MEMORIES IN EINER CONTROLLER-ARCHITEKTUR SOWIE EIN ENTSPRECHENDES COMPUTERPROGRAMMPRODUKT UND EIN ENTSPRECHENDES COMPUTERLESBARES SPEICHERMEDIUM

(57) Abstract: The invention relates to a method and a system for writing NV memories in a controller architecture, in addition to a corresponding computer program product and a corresponding computer-readable storage medium, which can be used in particular to accelerate writing or programming operations in NV code memories of microcontrollers, such as e.g. smartcard controllers. The method consists of extending the instruction set of the controller by MOVCWR (move code write) instructions, which allow a defined data item (byte) to be written to a defined target address in an NV code memory. The data item (byte) is written to the correct position of the cache page register of the relevant NV memory and the page-address pointer register of the memory is updated with the corresponding page address. If an MMU (Memory Management Unit) is present, the MOVCWR write operation to the cache page register, in addition to the MOVC read or code fetch operation are controlled by said MMU.

(57) Zusammenfassung: Die Erfindung beschreibt ein Verfahren und eine Anordnung zum Beschreiben von NV-Memories in einer Controller-Architektur sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes computerlesbares Speichermedium, die insbesondere genutzt werden können, um Schreib- bzw. Programmiervorgänge in NV-Code-Memories von Mikrocontrollern, wie beispielsweise Smartcard-Controllern, zu beschleunigen. Das Verfahren besteht in einer Erweiterung des Befehlssatzes des Controllers um sog. MOVCWR (move code write)-Instruktionen, die es ermöglichen, ein definiertes Datenwort (Byte) an eine definierte Zieladresse innerhalb eines NV-Code-Memories zu schreiben. Das Datenwort (Byte) wird hierbei an die korrekte Position des Cache-Pageregisters des jeweiligen NV-Memories geschrieben und die Pageadreß-Pointerregister des Memories mit der zugehörigen Pageadresse aktualisiert. Wenn eine MMU (Memory Management Unit) vorhanden ist, geschieht dieses MOVCWR-Schreiben in das Cache-Pageregister, wie das MOVC-Lesen bzw. der Code-Fetch, unter Kontrolle dieser MMU.

WO 03/060721 A2

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und Anordnung zum Beschreiben von NV-Memories in einer Controller-Architektur sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes computerlesbares Speichermedium

Die Erfindung betrifft ein Verfahren und eine Anordnung zum Beschreiben von NV-Memories in einer Controller-Architektur sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes computerlesbares Speichermedium, die insbesondere genutzt werden können, um Schreib- bzw. Programmiervorgänge in NV-Code-Memories von Mikrocontrollern, wie beispielsweise Smartcard-Controllern, zu beschleunigen.

Die Entwicklung der Mikroelektronik in den 70er-Jahren ermöglichte es, kleine Computer im Kreditkartenformat ohne Benutzungsschnittstelle herzustellen. Solche Computer werden als Smartcards bezeichnet. In einer Smartcard sind Datenspeicher und arithmetisch-logische Einheiten in einem einzigen Chip von wenigen Quadratmillimetern Größe integriert. Smartcards werden insbesondere als Telefonkarten, GSM-SIM-Karten, im Bankenbereich und im Gesundheitswesen eingesetzt. Die Smartcard ist damit zur allgegenwärtigen Rechenplattform geworden.

Smartcards werden derzeit vornehmlich als sicherer Aufbewahrungsort für geheime Daten und als sichere Ausführungsplattform für kryptographische Algorithmen betrachtet. Die Annahme einer relativ hohen Sicherheit der Daten und Algorithmen auf der Karte liegt im Hardwareaufbau der Karte und den nach außen geführten Schnittstellen begründet. Die Karte stellt sich nach außen als "Black Box" dar, deren Funktionalität nur über eine wohldefinierte Hardware- und Softwareschnittstelle in Anspruch genommen werden kann, und die bestimmte Sicherheitspolicies erzwingen kann. Zum einen kann der Zugriff auf Daten an bestimmte Bedingungen geknüpft werden. Kritische Daten, wie zum Beispiel geheime Schlüssel eines Public-Key-Verfahrens, können dem Zugriff von außen sogar völlig entzogen werden. Zum anderen ist eine Smartcard in der Lage, Algorithmen auszuführen, ohne daß die Ausführung der einzelnen Operationen von außen beobachtet werden kann. Die Algorithmen selbst können auf der Karte vor Veränderung und Auslesen geschützt werden. Im objektorientierten Sinn läßt sich die Smartcard als abstrakter Datentyp auffassen, der über eine wohldefinierte Schnittstelle verfügt, ein spezifiziertes Verhalten

aufweist und selbst in der Lage ist, die Einhaltung bestimmter Integritätsbedingungen bezüglich seines Zustandes sicherzustellen.

Es gibt im Wesentlichen zwei verschiedene Typen von Smartcards. Speicherkarten besitzen lediglich eine serielle Schnittstelle, eine Adressierungs- und Sicherheitslogik und ROM- und EEPROM-Speicher. Diese Karten besitzen nur eingeschränkte Funktionalität und dienen einer spezifischen Anwendung. Dafür sind sie besonders billig herzustellen. Als Mikroprozessorkarten hergestellte Smartcards stellen im Prinzip einen vollständigen Universalrechner dar.

Der Herstellungs- und Auslieferungsprozeß für Chipkarten gliedert sich in folgende Phasen:

- Herstellen des Halbleiters,
- Einbetten des Halbleiters,
- Bedrucken der Karte,
- Personalisierung der Karte,
- Ausgeben der Karte.

Im Allgemeinen wird jede Phase von einer auf die jeweilige Arbeit spezialisierten Firma durchgeführt. Beim Herstellen der Halbleiter ist insbesondere bei Karten mit festverdrahteter Sicherheitslogik auf eine gute betriebsinterne Sicherheit zu achten. Damit vom Hersteller ein korrekter Endtest durchgeführt werden kann, muß der komplette Speicher frei zugänglich sein. Erst nach dem Endtest wird der Chip durch einen Transportcode gesichert. Danach ist der Zugriff auf den Kartenspeicher nur für berechtigte Stellen, die den Transportcode kennen, möglich. Ein Diebstahl fabrikneuer Halbleiter bleibt damit ohne Folgen. Berechtigte Stellen können Personalisierer bzw. Kartenausgeber sein. Für das Einbetten und Bedrucken sind keine weiteren Sicherungsfunktionen notwendig. Die betreffenden Firmen brauchen den Transportcode nicht zu kennen.

Im allgemeinen überträgt nicht der Kartenhersteller, sondern die ausgebende Stelle (zum Beispiel Bank, Telefongesellschaft, Krankenkasse etc.) die personenspezifischen Daten in die Karte. Diesen Vorgang nennt man Personalisierung. Für sie ist die Kenntnis des Transportcodes notwendig.

Das Ausgeben der Karte, also der Transport von der ausgebenden Stelle zum Karteninhaber, stellt ein weiteres Sicherheitsproblem dar. Genau genommen ist nur die persönliche Ausgabe an den Karteninhaber gegen Unterschrift und Vorlage des Personalausweises sicher. Ein Versand per Post ist zwar oft wirtschaftlicher, aber auch

ziemlich unsicher. Ein Problem ist auch das Übermitteln der PIN an den Karteninhaber, hier muß die gleiche Sorgfalt wie für die Karte gelten.

Bedingt durch die brisanten, sicherheitsrelevanten Inhalte der auf Smartcard-Controllern befindlichen Speicher ist neben der Beachtung dieser Sicherungsmaßnahmen ein zusätzlicher Schutz gegen mögliche Aktivitäten von Hackern zu gewährleisten, die sich auf alle Phasen des Lebenslaufes einer Smartcard - beginnend von der Herstellung, über Transport, Nutzung der Karte bis zu Manipulationen unbrauchbar gewordener Karten - erstrecken.

Bei der Programmierung von größeren Mengen von Daten/Code in NV-Memories (zum Beispiel bei der Personalisierung in das EEPROM) entsteht ein relativ großer Zeitverlust einerseits durch den Datentransport via SFR-Bus, andererseits durch die notwendige Verifikation der geschriebenen EEPROM-Daten nach dem Programmieren jeder Page.

Zur Zeit bieten die Standard-Befehlssätze von Controllern für den Code-Memory-Bereich ausschließlich lesende Instruktionen. D.h., aus NV-Memories können Daten entweder als Instuction-Code abgerufen oder als Datenwort („Byte") durch eine sog. MOVC-Instruktion gelesen werden.

Ein Beschreiben/Programmieren von Daten in das NV-Memory erfolgte bisher ausschließlich über den Registersatz des jeweiligen Memory-Interfaces, d.h., der Datenweg beim Beschreiben des NV-Memories ist komplett getrennt vom Datenweg des Code-Fetch / MOVC-Lesens.

Das Beschreiben erfordert mehrere Schreibzugriffe auf Memory-Interface-Register: Beschreiben der Adreß-Register für Page-Adresse und Byte-Adresse, Beschreiben des Daten-Registers und des Kontroll-Registers.

Das bisherige Verfahren zum Beschreiben von NV-Memories ist gegenüber dem Code-Fetch/Lesen sehr langsam, da es je nach Zugriffsart zwei bis fünf Registerzugriffe pro geschriebenem Datenwort erfordert, während Code-Fetch und MOVC-Lesen im schnellen Code-Fetch-Takt des Prozessors ablaufen.

Da das Schreiben hierbei ausschließlich über die Register-Schnittstelle des Memory-Interfaces läuft, hat die Memory-Management-Unit, die das Mapping und die Zugriffsrechte des Code-Memories insgesamt kontrolliert, beim Beschreiben des NV-Memories keinen Einfluß. Daher kann das Beschreiben des Memories nur unter Kontrolle des Operating-Systems des Controllers geschehen und ist für Applikations-SW nur durch spezielle Calls auf System-Routinen möglich.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren, eine Anordnung sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes computerlesbares Speichermedium der gattungsgemäßen Art anzugeben, durch welche die Nachteile der herkömmlichen Vorgehensweisen vermieden werden und durch welche es ermöglicht wird, in kürzestmöglicher Zeit Daten in ein NV-Memory zu schreiben, ohne wesentliche Eingriffe in bisher benutzten Verfahren vornehmen zu müssen, sowie einen höheren Schutz vor Programmierfehlern zu gewährleisten.

Erfindungsgemäß wird diese Aufgabe gelöst durch die Merkmale im kennzeichnenden Teil der Ansprüche 1, 12, 14 und 15 im Zusammenwirken mit den Merkmalen im Oberbegriff. Die Unteransprüche enthalten zweckmäßige Ausgestaltungen der Erfindung.

Ein besonderer Vorteil des Verfahrens zum Beschreiben von NV-Memories in einer Controller-Architektur besteht darin, daß (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Page-Address-Pointerregister des NV-Memories aktualisiert werden.

Eine Anordnung zum Beschreiben von NV-Memories in einer Controller-Architektur ist vorteilhafterweise so eingerichtet, daß sie einen Prozessor umfaßt, der derart eingerichtet ist, daß ein Beschreiben von NV-Memories in einer Controller-Architektur durchführbar ist, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Page-Address-Pointerregister des NV-Memories aktualisiert werden.

Ein Computerprogrammprodukt zum Beschreiben von NV-Memories in einer Controller-Architektur umfaßt ein computerlesbares Speichermedium, auf dem ein Programm gespeichert ist, das es einem Computer oder Smartcard-Controller ermöglicht, nachdem es in den Speicher des Computers oder des Smartcard-Controllers geladen worden ist, ein Beschreiben von NV-Memories in einer Controller-Architektur durchzuführen, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-

Pageregisters des NV-Memories geschrieben werden (wird) und die Page-Address-Pointerregister des NV-Memories aktualisiert werden.

Um ein Beschreiben von NV-Memories in einer Controller-Architektur durchzuführen, wird vorteilhaft ein computerlesbares Speichermedium eingesetzt, auf dem ein Programm gespeichert ist, das es einem Computer oder Smartcard-Controller ermöglicht, nachdem es in den Speicher des Computers oder des Smartcard-Controllers geladen worden ist, das Beschreiben von NV-Memories in einer Controller-Architektur durchzuführen, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Page-Address-Pointerregister des NV-Memories aktualisiert werden.

Vorteilhaft wird ferner zum Beschreiben des NV-Memories der Befehlssatz des Controller-Cores um zusätzliche Move-Code-Write-Instruktionen (MOVCWR-Instruktionen) erweitert. In bevorzugter Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, daß die zusätzlichen Instruktionen des Controller-Cores eine Übergabe der Parameter für Adreß-Pointer und für den zu schreibenden Datenwert oder das zu schreibende Datenwort durchführen und entsprechende Kontrollsignale für eine sog. Memory-Management-Unit (MMU) und NV-Memory-Interfaces aktivieren.

Als vorteilhaft erweist es sich, daß bei Vorhandensein einer Memory-Management-Unit (MMU) die Adreßverarbeitung für die MOVCWR-Instruktionen in gleicher Weise erfolgt wie die Verarbeitung von Code-Fetches oder MOVC-Instruktionen. Darüber hinaus ist in bevorzugter Ausgestaltung des erfindungsgemäßen Verfahrens vorgesehen, daß bei Vorhandensein einer Memory-Management-Unit (MMU) des Controllers diese MMU um einen Kontrollsignalpfad erweitert wird.

Vorteilhaft werden bei Vorhandensein einer MMU nur Adreßbereiche des NV-Memories beschrieben, die von der MMU freigegeben sind. Zum Beschreiben von NV-Memories in einer Controller-Architektur kann es sich als vorteilhaft erweisen, daß bei Vorhandensein einer MMU ein spezielles Mapping des Code Memories innerhalb des Adreßbereichs des Controllers berücksichtigt wird.

In weiterer bevorzugter Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, daß nacheinander mehrere Datenwerte und/oder Datenworte mit derselben Pageadresse geschrieben werden.

Vorteilhaft wird durch Beschreiben des Control-Registers des NV-Memories der Inhalt des Cache-Page-Registers in das NV-Memory programmiert. Darüber hinaus ist in bevorzugter Ausgestaltung des erfindungsgemäßen Verfahrens vorgesehen, daß beim Wechsel auf eine neue Pageadresse bei einer MOVCWR-Instruktion das Cache-Page-Register des NV-Memories gelöscht wird.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, daß ein ungewolltes Programmieren alter Page-Register-Inhalte unter falscher Adresse verhindert wird. Darüber hinaus ist in bevorzugter Ausgestaltung der erfindungsgemäßen Anordnung vorgesehen, daß der Prozessor Teil eines Smartcard-Controllers und die Anordnung eine Smartcard ist.

Das erfindungsgemäße Verfahren bietet gegenüber dem bisher rein durch das Register-Interfaces des NV-Memories unterstützten Beschreiben des Cache-Pageregister mehrere Vorteile.

Das Beschreiben des NV-Memories mit MOVCWR erfordert pro Datenwort (Byte) nur eine MOVCWR-Instruktion mit Übergabe der beiden Parameter für den Adreßpointer und das Datenwort. Bei mehreren aufeinander folgenden MOVCWR-Instruktionen kann wie beim MOVC-Lesen ein „Autoincrement" des Adreßpointers benutzt werden. Dieser Befehlsaufruf stellt eine erhebliche Beschleunigung des Schreibvorganges gegenüber dem Schreiben via Adreß/Daten-Registersatz des NV-Memories da.

Spezielle Adreßbereichs-Mappings oder Zugriffs-Einschränkungen des Code-Memories, die von einer eventuell vorhandenen MMU überwacht werden, sind für MOVCWR auf gleiche Weise gültig wie für Code-Fetch und MOVC, d.h., der Prozessor-Core sieht bei der Ausführung von MOVCWER das gleiche Memory-Mapping wie bei Code-Fetch / MOVC.

Daher ist es auch einer Applikations-SW möglich, direkt die MOVCWR-Instruktion zu verwenden, um das Cache-Pageregister eines NV-Memories zu beschreiben, ohne einen System-Call aufrufen zu müssen. Die Kontrolle über die Zugriffsrechte auf das Memory behält das OS des Controllers über die Konfiguration der MMU Kontroll-Register.

Ein fehlerhaftes Programmieren alter Inhalte des Cache-Page-Registers eines NV-Memories an eine falsche Pageadresse ist nicht mehr möglich, da das Cache-Page-Register mit jedem MOVCWR, dessen Adreß-Pointer die Pageadresse ändert, zurückgesetzt wird.

Die Erfindung wird nachfolgend in einem Ausführungsbeispiel näher erläutert.

Das vorgestellte Verfahren besteht in einer Erweiterung des Befehlssatzes des Controllers um sog. MOVCWR (move code write) Instruktionen, die es ermöglichen, ein definiertes Datenwort (Byte) an eine definierte Zieladresse innerhalb eines NV-Code-Memories zu schreiben. Das Datenwort (Byte) wird hierbei an die korrekte Position des Cache-Pageregisters des jeweiligen NV-Memories geschrieben und die Pageadreß-Pointerregister des Memories mit der zugehörigen Pageadresse aktualisiert.

Wenn bei advanced Smartcard-Controllern eine MMU (Memory Management Unit) vorhanden ist, geschieht dieses MOVCWR-Schreiben in das Cache-Pageregister, wie das MOVC-Lesen bzw. der Code-Fetch, unter voller Kontrolle dieser MMU, so daß nur auf Adreßbereiche des Speichers geschrieben werden kann, die grundsätzlich von der MMU dafür freigegeben sind. Spezielles Mapping des Code Memories innerhalb des Adreßbereiches des Controllers wird hierbei berücksichtigt.

Auf diese Weise können nacheinander mehrere Bytes/Worte mit derselben Pageadresse geschrieben werden, um das Cache-Pageregister zu füllen. Durch Beschreiben des Control-Registers des jeweiligen NV-Memories kann dann der Inhalt des Cache-Page-Registers in das NV-Memory programmiert werden.

Jeder Wechsel auf einer neuen Pageadresse bei einer MOVCWR-Instruktion hat ein sofortiges Löschen des Cache-Pageregisters des NV-Memories zur Folge, um ein Programmieren von Daten unter der neuen Pageadresse zu ermöglichen und ein ungewolltes Programmieren alter Pageregister-Inhalte unter falscher Adresse zu verhindern.

In der beispielhaften Ausführungsform wird der Befehlssatz des Controller-Cores um zusätzliche MOVCWR-Instruktionen erweitert, um das Beschreiben von NV-Memories in erfindungsgemäßer Weise auszuführen. Die zusätzlichen MOVCWR-Instruktionen gewährleisten die eine Übergabe der Parameter für den Adreß-Pointer und den zu schreibenden Datenwert und aktivieren entsprechende Kontrollsignale für MMU und Memory-Interfaces.

Eine eventuell vorhandene MMU (Memory Management Unit) des Controllers wird erweitert um einen entsprechenden Kontrollsignal-Pfad, der bei der Ausführung der MOVCWR Instruktion die entsprechenden Chip-Select-Signale für die Memory-Interfaces generiert. Die Adreßverarbeitung für die MOVCWR Instruktionen (bez. Mapping und Access Rights) unterscheidet sich hierbei nicht von der Verarbeitung von Code-Fetches oder MOVC-Instruktionen.

Die Memory-Interfaces der NV-Memories unterstützen diese Funktion durch einen entsprechenden Write-Mode für die Cache-Pageregister und einer

Aktualisierungsfunktion der Adreß-Register nach jedem MOVCWR Vorgang. Außerdem führt eine Reset-Logik vor jedem MOVCWR-Vorgang einen Adreßvergleich zwischen alter und neuer Pageadresse durch und löst gegebenenfalls bei einem Adreßwechsel vor dem Beschreiben des Cache-Pageregisters ein Löschen des alten Registerinhaltes aus.

Die Erfindung ist nicht beschränkt auf die hier dargestellten Ausführungsbeispiele. Vielmehr ist es möglich, durch Kombination und Modifikation der genannten Mittel und Merkmale weitere Ausführungsvarianten zu realisieren, ohne den Rahmen der Erfindung zu verlassen.

PATENTANSPRÜCHE:

1. Verfahren zum Beschreiben von NV-Memories in einer Controller-Architektur,
dadurch gekennzeichnet, daß (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Pageadreß-Pointerregister des NV-Memories aktualisiert werden.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß zum Beschreiben des NV-Memories der Befehlssatz des Controller-Cores um zusätzliche Move-Code-Write-Instruktionen (MOVCWR-Instruktionen) erweitert wird.

3. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß die zusätzlichen Instruktionen des Controller-Cores eine Übergabe der Parameter für Adreß-Pointer und für den zu schreibenden Datenwert oder das zu schreibende Datenwort durchführen und entsprechende Kontrollsignale für eine Memory-Management-Unit (MMU) und NV-Memory-Interfaces aktivieren.

4. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß bei Vorhandensein einer Memory-Management-Unit (MMU) die Adreßverarbeitung für die MOVCWR-Instruktionen in gleicher Weise erfolgt wie die Verarbeitung von Code-Fetches oder MOVC-Instruktionen.

5. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß bei Vorhandensein einer Memory-Management-Unit (MMU) des Controllers diese MMU um einen Kontrollsignal-Pfad erweitert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, daß bei Vorhandensein einer MMU nur Adreßbereiche des NV-Memories beschrieben werden, die von der MMU freigegeben sind.

7. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß bei Vorhandensein einer MMU ein spezielles Mapping des Code Memories innerhalb des Adreßbereichs des Controllers berücksichtigt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß nacheinander mehrere Datenwerte und/oder Datenworte mit derselben Pageadresse geschrieben werden.

9. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß durch Beschreiben des Control-Registers des NV-Memories der Inhalt des Cache-Page-Registers in das NV-Memory programmiert wird.

10. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß beim Wechsel auf eine neue Pageadresse bei einer MOVCWR-Instruktion das Cache-Page-Register des NV-Memories gelöscht wird.

11. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß ein ungewolltes Programmieren alter Page-Register-Inhalte unter falscher Adresse verhindert wird.

12. Anordnung mit einem Prozessor, der derart eingerichtet ist, daß ein Beschreiben von NV-Memories in einer Controller-Architektur durchführbar ist, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Pageadreß-Pointerregister des NV-Memories aktualisiert werden.

13. Anordnung mit einem Prozessor nach Anspruch 12,
dadurch gekennzeichnet, daß der Prozessor Teil eines Smartcard-Controllers und die Anordnung eine Smartcard ist.

14. Computerprogrammprodukt, das ein computerlesbares Speichermedium umfaßt, auf dem ein Programm gespeichert ist, das es einem Computer oder Smartcard-Controller ermöglicht, nachdem es in den Speicher des Computers oder des Smartcard-Controllers geladen worden ist, ein Beschreiben von NV-Memories in einer Controller-Architektur durchzuführen, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Pageadreß-Pointerregister des NV-Memories aktualisiert werden.

15. Computerlesbares Speichermedium, auf dem ein Programm gespeichert ist, das es einem Computer oder Smartcard-Controller ermöglicht, nachdem es in den Speicher des Computers oder des Smartcard-Controllers geladen worden ist, ein Beschreiben von NV-Memories in einer Controller-Architektur durchzuführen, wobei (ein) definierte(r) Datenwert(e) oder (ein) definierte(s) Datenwort(e) an (eine) definierte Zieladresse(n) innerhalb des NV-Memories geschrieben werden (wird), indem die (der) Datenwert(e) bzw. die (das) Datenwort(e) an die vorgegebene Position des Cache-Pageregisters des NV-Memories geschrieben werden (wird) und die Pageadreß-Pointerregister des NV-Memories aktualisiert werden.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
24. Juli 2003 (24.07.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2003/060721 A3

(51) Internationale Patentklassifikation[7]: G06F 12/02

(21) Internationales Aktenzeichen: PCT/IB2002/005481

(22) Internationales Anmeldedatum:
12. Dezember 2002 (12.12.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 64 422.1 29. Dezember 2001 (29.12.2001) IB

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von DE, SI, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Anmelder *(nur für DE)*: **PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BUHR, Wolfgang** [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MUELLER, Detlef** [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Anwalt: **PETERS, Carl, H.**; Philips Intellectual Property & Standards, Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 13. Mai 2004

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: METHOD AND SYSTEM FOR WRITING NV MEMORIES IN A CONTROLLER ARCHITECTURE, CORRESPONDING COMPUTER PROGRAM PRODUCT AND COMPUTER-READABLE STORAGE MEDIUM

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUM BESCHREIBEN VON NV-MEMORIES IN EINER CONTROLLER-ARCHITEKTUR SOWIE EIN ENTSPRECHENDES COMPUTERPROGRAMMPRODUKT UND EIN ENTSPRECHENDES COMPUTERLESBARES SPEICHERMEDIUM

(57) Abstract: The invention relates to a method and a system for writing NV memories in a controller architecture, in addition to a corresponding computer program product and a corresponding computer-readable storage medium, which can be used in particular to accelerate writing or programming operations in NV code memories of microcontrollers, such as e.g. smartcard controllers. The method consists of extending the instruction set of the controller by MOVCWR (move code write) instructions, which allow a defined data item (byte) to be written to a defined target address in an NV code memory. The data item (byte) is written to the correct position of the cache page register of the relevant NV memory and the page-address pointer register of the memory is updated with the corresponding page address. If an MMU (Memory Management Unit) is present, the MOVCWR write operation to the cache page register, in addition to the MOVC read or code fetch operation are controlled by said MMU.

(57) Zusammenfassung: Die Erfindung beschreibt ein Verfahren und eine Anordnung zum Beschreiben von NV-Memories in einer Controller-Architektur sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes computerlesbares Speichermedium, die insbesondere genutzt werden können, um Schreib- bzw. Programmiervorgänge in NV-Code-Memories von Mikrocontrollern, wie beispielsweise Smartcard-Controllern, zu beschleunigen. Das Verfahren besteht in einer Erweiterung des Befehlssatzes des Controllers um sog. MOVCWR (move code write)-Instruktionen, die es ermöglichen, ein definiertes Datenwort (Byte) an eine definierte Zieladresse innerhalb eines NV-Code-Memories zu schreiben. Das Datenwort (Byte) wird hierbei an die korrekte Position des Cache-Pageregisters des jeweiligen NV-Memories geschrieben und die Pageadreß-Pointerregister des Memories mit der zugehörigen Pageadresse aktualisiert. Wenn eine MMU (Memory Management Unit) vorhanden ist, geschieht dieses MOVCWR-Schreiben in das Cache-Pageregister, wie das MOVC-Lesen bzw. der Code-Fetch, unter Kontrolle dieser MMU.

WO 2003/060721 A3

INTERNATIONAL SEARCH REPORT

PCT/IB 02/05481

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Xilinx Generic Flash Memory Interface Solutions" XILINX WHITE PAPER, vol. WP143, no. v1.0, 8 May 2001 (2001-05-08), page 1-12 XP002268172 page 11; figure 9	1-15

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 2004	12/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weber, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Continuation of I.2

Claims: all 1-15

In view of the fact that the current claims contain the terms "cache page register" and "page address point register", which are neither standard terms nor anywhere defined in the description, and hence make it impossible to determine the scope of protection sought, the present application does not meet the requirements of PCT Article 6, and so a meaningful search is not feasible.

The applicant is advised that claims or parts of claims relating to inventions in respect of which no international search report has been established normally cannot be the subject of an international preliminary examination (PCT Rule 66.1(e)). In its capacity as International Preliminary Examining Authority the EPO generally will not carry out a preliminary examination for subjects that have not been searched. This also applies to cases where the claims were amended after receipt of the international search report (PCT Article 19) or where the applicant submits new claims in the course of the procedure under PCT Chapter II.

INTERNATIONALER RECHERCHENBERICHT

PCT/IB 02/05481

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F12/02

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	"Xilinx Generic Flash Memory Interface Solutions" XILINX WHITE PAPER, Bd. WP143, Nr. v1.0, 8. Mai 2001 (2001-05-08), Seite 1-12 XP002268172 Seite 11; Abbildung 9	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. Januar 2004	12/02/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weber, R

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen PCT/IB 02 05481

WEITERE ANGABEN PCT/ISA/ 210

Fortsetzung von Feld I.2

Ansprüche Nr.: alle 1-15

Angesicht die Ausdrücke "Cache-Pageregister" and "Pageadress-Pointerregister" der geltenden Patentansprüche weder in der ganzen Beschreibung definiert noch Standardausdrücke sind und damit es unmöglich machen, den durch sie erstrebten Schutzumfang zu bestimmen, entspricht die vorliegende Patentanmeldung den Anforderungen des Artikels 6 PCT nicht, so daß eine sinnvolle Recherche undurchführbar ist.

Der Anmelder wird darauf hingewiesen, daß Patentansprüche, oder Teile von Patentansprüchen, auf Erfindungen, für die kein internationaler Recherchenbericht erstellt wurde, normalerweise nicht Gegenstand einer internationalen vorläufigen Prüfung sein können (Regel 66.1(e) PCT). In seiner Eigenschaft als mit der internationalen vorläufigen Prüfung beauftragte Behörde wird das EPA also in der Regel keine vorläufige Prüfung für Gegenstände durchführen, zu denen keine Recherche vorliegt. Dies gilt auch für den Fall, daß die Patentansprüche nach Erhalt des internationalen Recherchenberichtes geändert wurden (Art. 19 PCT), oder für den Fall, daß der Anmelder im Zuge des Verfahrens gemäß Kapitel II PCT neue Patentansprüche vorlegt.

INTERNATIONALER RECHERCHENBERICHT

PCT/IB 02/05481

Feld I Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche die Behörde nicht verpflichtet ist, nämlich

2. ☒ Ansprüche Nr. alle 1-15
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, daß eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich
siehe Zusatzblatt WEITERE ANGABEN PCT/ISA/210

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefaßt sind.

Feld II Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere Erfindungen enthält:

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☐ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:

Bemerkungen hinsichtlich eines Widerspruchs

☐ Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt.

☐ Die Zahlung zusätzlicher Recherchengebühren erfolgte ohne Widerspruch.